LISTING OF THE CLAIMS

1. (Cancelled)

2. (Cancelled)

3. (Cancelled)

4. (Cancelled)

5. (Cancelled)

6. (Cancelled)

7. (Cancelled)

8. (Cancelled)

9. (Previously Amended) A computer network intrusion detection system comprising:

a plurality of different log analyzers for different external networks, each log analyzer being configured for detecting attacks upon a firewall in an corresponding one of the different external networks defining an edge detection network;

an edge database log coupled to the different log analyzers logging attacks upon the different external networks;

an intrusion detector coupled to a client network and configured to detect external attacks upon the client network;

an analyzer coupled to said intrusion detector for analyzing each detected attack and determining a characteristic indicative thereof to classify each detected attack as a general attack or a client specific attack based upon logged attacks in the edge database log; and,

a filter coupled to said analyzer for generating an alert based upon characteristics of a plurality of attacks;

a second intrusion detector for detecting external attacks upon a second computer network; and,

a second analyzer coupled to said second intrusion detector for analyzing each detected attack upon the second network and determining a characteristic indicative thereof, wherein said filter is further coupled to said second analyzer and further compares the attack characteristics determined by said analyzer and said second analyzer and generates a specific attack alert in response to a substantial absence of similarity in the comparison.

10. (Original) The system according to claim 9 further comprising an alert generator for generating an alert indicative of the specific attack on the one of the networks experiencing the attacks having the absence of similarity of attacks on the other of the networks.

11. (Original) The system according to claim 9 further comprising: a vulnerability tester coupled to said filter for testing the one of the networks not experiencing the attacks for a vulnerability to the attack characteristic experienced by the other of the computer networks.

12. (Cancelled)

13. (Cancelled)

14. (Currently Amended) A method of generating a network intrusion alert for a first network coupled to a multiple client network system comprising the steps of:

logging attacks on multiple different external networks defining an edge detection network;

detecting an attack on a client network;

classifying the attack as either a general attack or a client specific attack by comparing the attack to attacks logged for the edge detection network;

prioritizing handling of the detected attack if the attack is classified as a general attack; ~~and,~~

generating a first alert in response to an absence of a match between the attack and the attacks logged for the edge detection network, wherein the first alert is indicative of a client specific attack on the first network; and

generating a second alert in response to ~~the~~ a presence of ~~the~~ a match between the attack and the attacks logged for the edge detection network, wherein the ~~first alert is indicative of a specific attack on the first network and the~~ second alert is indicative of a ~~non-specific~~ general attack on the first network.

15. (Cancelled)

16. (Cancelled)

17. (Cancelled)

18. (Cancelled)

19. (Cancelled)

20. (Cancelled)